

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

13.03.00

REC'D 28 APR 2000

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 2月22日

Eku

出 願 番 号

Application Number:

平成11年特許願第043870号

出 願 人

Applicant(s):

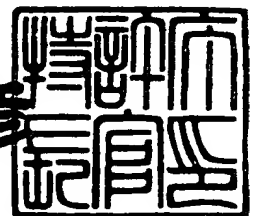
松下電器産業株式会社

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 4月14日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



出証番号 出証特2000-3025745

【書類名】 特許願

【整理番号】 2054001393

【提出日】 平成11年 2月22日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/00  
G06F 11/34

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 武知 秀明

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山田 正純

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 飯塚 裕之

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 西村 拓也

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 久野 良樹

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 後藤 昌一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100092794

【弁理士】

【氏名又は名称】 松田 正道

【電話番号】 066397-2840

【手数料の表示】

【予納台帳番号】 009896

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9006027

【ブループの要否】 要

【書類名】 明細書

【発明の名称】 コンピュータ及びプログラム記録媒体

【特許請求の範囲】

【請求項 1】 システム部とアプリケーションソフトウェア部とを備え、  
デジタルインターフェースから著作権主張された暗号化データを取り込み、  
処理するコンピュータにおいて、  
前記システム部は、前記アプリケーションソフトウェア部が著作権を守る上において  
正当なアプリケーションソフトウェアであると判定し、  
正当なものである場合は、暗号化データの鍵をアプリケーションソフトウェア  
部に渡すことを特徴とするコンピュータ。

【請求項 2】 前記システム部における判定は、前記システム部とアプリケーション  
ソフトウェア部との間における認証で行われることを特徴とする請求項 1  
記載のコンピュータ。

【請求項 3】 前記システム部における判定は、不正なまたは正当なアプリケーション  
ソフトウェアが載っている CRL (Certification Revocation List) で行うことを特徴とする請求項 1 記載のコンピ  
ュータ。

【請求項 4】 前記システム部は前記暗号化された鍵を外部との認証結果によ  
り得て、前記暗号化されたデータを復号し、再度その鍵または別の鍵で復号化さ  
れたデータを再暗号化することを特徴とする請求項 1～3 のいずれかに記載のコン  
ピュータ。

【請求項 5】 前記システム部はタンパ確認関数を有しており、前記アプリケ  
ーションソフトウェア部のアプリケーションソフトウェアにタンパコードが埋め  
込まれており、前記システム部は前記アプリケーションソフトウェア部からタン  
パコードを読みとり、タンパ確認関数を用いて、アプリケーションソフトウェア  
の改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は  
、その結果を知らせることを特徴とする請求項 1～4 のいずれかに記載のコンピ  
ュータ。

【請求項 6】 システム部とアプリケーションソフトウェア部とを備え、

デジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は複数種類のタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアには所定の種類のタンパ確認関数に対応するタンパコードとその種類情報が埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードとその種類情報を読み取り、その種類に対応するタンパ確認関数を用いて、アプリケーションソフトウェアの改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とするコンピュータ。

【請求項 7】 システム部とアプリケーションソフトウェア部とを備え、

デジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は、前記アプリケーションソフトウェア部のアプリケーションソフトウェアに関する情報を前記データに埋め込んで前記データをアプリケーション部へ送ることを特徴とするコンピュータ。

【請求項 8】 前記アプリケーションソフトウェアに関する情報とは、前記アプリケーションソフトウェアの名前、または前記アプリケーションソフトウェアのバージョン番号、またはタンパコード、またはタンパレジスタンス確認関数の種類情報、または使用者に関する情報であることを特徴とする請求項 7 記載のコンピュータ。

【請求項 9】 請求項 1～8 のいずれかに記載のコンピュータの各構成要素の全部または一部の機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データを記録再生するコンピュータ及びプログラム記録媒体に関するものである。

【0002】

## 【従来の技術】

音声情報や映像情報をデジタル化して伝送するネットワークが開発されてきている。音声情報や映像情報を伝送し、視聴するためにはリアルタイムにデータを伝送する必要がある。

## 【0003】

このようなリアルタイムデータ伝送を行うネットワークの標準としてIEEE 1394が提案され、現在広く用いられるようになった。IEEE 1394は、家庭用デジタルVCRを始め、多くのデジタル映像音声機器に外部用インターフェースとして搭載されている。VCRにおいては、IEEE 1394を用いることにより、外部機器からVCRの動作制御を行ったり、また外部機器からVCRにデータを送信し、VCRにおいて記録することや再生することなども可能となった。

## 【0004】

一方PCにおいては、マルチメディア技術の進展、大容量のハードディスクや光磁気ディスクなどの記録媒体の出現により、映像情報や音声情報をも処理できるようになった。すなわちPCは映像情報や音声情報の記録再生装置やモニタとしても機能できるようになった。PCの標準OSであるWindows 98などにおいてはIEEE 1394がサポートされており、VCRなどのデジタル映像音声機器とPCで互いにAVデータのやりとりが可能となっている。このように今後デジタル映像音声機器とPCとの融合がますます進展していくものと思われる。

## 【0005】

PCで映像情報や音声情報を扱うためには、映像情報や音声情報を処理するアプリケーションソフトウェアをPCにインストールしておく必要がある。映像音声機器から送られてくるAVデータはPCの内部に入力され、PCにインストールされているアプリケーションソフトウェアによって表示、記録、再生などの処理が行われる。例えばアプリケーションソフトウェアが記録を行う機能を持つものであれば、映像音声機器から送られてきたAVデータはPCに入力され、アプリケーションソフトウェアによって、ハードディスクや光磁気ディスクなどの記

録媒体に記録される。このようにAVデータを処理できるアプリケーションソフトウェアは様々であり、アプリケーションソフトウェアをインストールすることによってPCにAVデータを処理するための記録、再生、表示、加工など多種多様な機能を付加することができる。

【0006】

一方AVデータには複製を禁止する、一世代のみ複製を許可するなどの著作権主張されたAVデータがある。このように著作権主張されたAVデータはVCRなどのデジタル映像音声機器ではその著作権の意図するところを守って記録、再生などが行われる。例えば複製を禁止するというAVデータに対してはVCRは記録をしない。ところが一世代のみ複製を許可するというAVデータであればVCRは記録することができる。このようにAVデータを複製できるか否かは、VCRとSTB（衛星放送受信器）などのAVデータの送り手となる機器との間で認証や著作権に基づく利用許諾情報によって確認する。

【0007】

【発明が解決しようとする課題】

しかし、現在のPCでは、著作権主張されたAVデータに対して、PCがその著作権を守ろうとしてもPCにインストールされているアプリケーションソフトウェアの機能によって、PCに記録、再生、表示などの多種多様の機能を持たせることが出来るため、著作権主張されたAVデータが一旦アプリケーションソフトウェアに渡されてしまえば、アプリケーションソフトウェアが自由にAVデータを記録などの任意の処理をすることが可能であり、著作権を守ることが出来ないという問題がある。

【0008】

また、アプリケーションソフトウェアに対して、著作権主張されたAVデータを処理するためのライセンスを付与する仕組みを作ったとしても、アプリケーションソフトウェアが不正に改竄されて、著作権が守られない場合がある。アプリケーションソフトウェアの不正改造を防ぐため、タンパレジスタントの方式をアプリケーションソフトウェアに実装すれば、効果的に著作権は守られる。しかしこの場合も一旦タンパレジスタントの方式が不正なユーザによって破られれば、

PCの構造やOS、アプリケーションソフトウェアの構成などを大きく変える必要が生じ、損失が大きいという問題がある。

## 【0009】

また、上述したようなライセンスを与えられていないアプリケーションソフトウェアが著作権主張されたデータを不正に扱った場合、不正なアプリケーションソフトウェアにより複製され流出したデータから出所のアプリケーションソフトウェアを特定することができない。すなわち不正なアプリケーションソフトウェアが知られた後、不正なアプリケーションソフトウェアを再び使おうとすると、それを検知し排斥することができない。つまり著作権保護に対して不正なソフトウェアを確認し、排斥することが不可能であるという問題がある。

## 【0010】

また、ソフトウェアによる不正利用の特徴はソフトウェアのコピー等により、不正利用の方法が低コストで広く流布し得ることである。そのため、たとえ不正流出の出所を特定できたとしても、ハードウェアの場合に用いられる不正な機器をその特定機器毎に排除する方式は有効でないという課題がある。例えばタンパレジスタントのチェックを回避出来る、改竄されたアプリケーションのコピーが流通したり、またはあるタンパレジスタントのチェック方式を回避する方法が、発見され流通した場合には、個別のコンピュータ毎に排除する従来の方式では不正を防止出来ない上、正常なアプリケーションさえ利用出来なくなる可能性がある。

## 【0011】

さらに、以上のような観点から、不正流出の仕組みを備えたコンピュータによる不正流出が一旦発覚した場合には、コンピュータやOS自体に対してAVデータの使用を禁止したり、コンピュータやOS自体の改変が必要になるなど広範囲に不利益が生じ、非常に大きなコストを要することは明らかである。

## 【0012】

このように、著作権主張されたデータが不正配布された場合に以後容易に不正利用を防止する方法がないという問題がある。

## 【0013】



本発明は、著作権主張されたデータに対してアプリケーションソフトウェアが著作権に反する処理を行うことが出来、著作権が守られないという課題と、アプリケーションソフトウェアが不正改造などにより、著作権主張に反することが行われるという課題と、不正なアプリケーションソフトウェアが発生した場合に、著作権保護に対して不正なアプリケーションソフトウェアを確認し、排斥することが不可能であるという課題と、タンパレジスタントのチェック方式を回避出来る改竄されたアプリケーションのコピーが流通した場合、従来の方式では不正を防止出来ないという課題と、不正流出の仕組みを備えたコンピュータによる不正流出が発覚した場合には、これを排除するために非常に大きなコストを要するという課題を考慮し、著作権主張されたデータに対しては著作権を守り、アプリケーションソフトウェアの不正な改竄に対処し、不正なアプリケーションソフトウェアに対して、そのアプリケーションソフトウェアを確認し、排斥し、不正な流出をコストをかけずに排除することができるコンピュータ及びプログラム記録媒体を提供することを目的とするものである。

## 【0014】

## 【課題を解決するための手段】

上述した課題を解決するために、第1の本発明（請求項1に対応）は、システム部とアプリケーションソフトウェア部とを備え、

ディジタルインターフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は、前記アプリケーションソフトウェア部が著作権を守る上において正当なアプリケーションソフトウェアであると判定し、

正当なものである場合は、暗号化データの鍵をアプリケーションソフトウェア部に渡すことを特徴とするコンピュータである。

## 【0015】

また第2の本発明（請求項2に対応）は、前記システム部における判定は、前記システム部とアプリケーションソフトウェア部との間における認証で行われることを特徴とする第1の発明に記載のコンピュータである。

## 【0016】

また第3の本発明（請求項3に対応）は、前記システム部における判定は、不正なまたは正当なアプリケーションソフトウェアが載っているCRL（Certification Revocation List）で行うことを特徴とする第1の発明に記載のコンピュータである。

## 【0017】

また第4の本発明（請求項4に対応）は、前記システム部は前記暗号化された鍵を外部との認証結果により得て、前記暗号化されたデータを復号し、再度その鍵または別の鍵で復号化されたデータを再暗号化することを特徴とする第1～3の発明のいずれかに記載のコンピュータである。

## 【0018】

また第5の本発明（請求項5に対応）は、前記システム部はタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアにタンパコードが埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードを読みとり、タンパ確認関数を用いて、アプリケーションソフトウェアの改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とする第1～4の発明のいずれかに記載のコンピュータである。

## 【0019】

また第6の本発明（請求項6に対応）は、システム部とアプリケーションソフトウェア部とを備え、

ディジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は複数種類のタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアには所定の種類のタンパ確認関数に対応するタンパコードとその種類情報が埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードとその種類情報を読み取り、その種類に対応するタンパ確認関数を用いて、アプリケーションソフトウェアの改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とするコンピュータである。

また第7の本発明（請求項7に対応）は、システム部とアプリケーションソフトウェア部とを備え、

デジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は、前記アプリケーションソフトウェア部のアプリケーションソフトウェアに関する情報を前記データに埋め込んで前記データをアプリケーション部へ送ることを特徴とするコンピュータである。

【0020】

また第8の本発明（請求項8に対応）は、前記アプリケーションソフトウェアに関する情報とは、前記アプリケーションソフトウェアの名前、または前記アプリケーションソフトウェアのバージョン番号、またはタンパコード、またはタンパレジスタンス確認関数の種類情報、または使用者に関する情報であることを特徴とする第7の発明に記載のコンピュータである。

【0021】

また第9の本発明（請求項9に対応）は、第1～8の発明のいずれかに記載のコンピュータの各構成要素の全部または一部の機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

【0022】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【0023】

（実施の形態1）

第1の実施の形態について図1、図7を参照して説明する。

【0024】

本実施の形態では、システム部とアプリケーションソフトウェア部とで認証を行い、またPCに入力されたAVデータは暗号化されてPCの内部を流通する場合を説明する。

【0025】

図1において、PC24は、システム部12とアプリケーションソフトウェア部13から構成される。システム部12は、PC24のD-I Fハードウェア内、またはドライバやOSなどのシステムソフトウェアである。アプリケーションソフトウェア部13は、アプリケーションソフトウェアを記録し、またアプリケーションソフトウェアを実行する手段である。

## 【0026】

システム部12は、1394 D-I F1、伝送認証手段2、アプリ認証関数3、署名メモリ4、伝送解読手段6、PC内用暗号化手段7から構成される。

## 【0027】

1394 D-I F1は、シリアルバスインターフェースの標準であるIEEE 1394のインターフェースであり、STBやD-VHSなどの外部機器とデータや、コマンドのやり取りを行うインターフェースである。伝送認証手段2は、AVデータが著作権主張されている場合、外部機器との間で認証を行い、認証が成功すると伝送解読手段6にAVデータを復号化するための鍵を渡す手段である。アプリ認証関数は、1394 D-I F1を介して入力されたAVデータが著作権主張されている場合PCの内部で認証を行う手段である。つまり署名生成手段9によって作成された署名を記録した署名メモリ4の内容を参照することによってアプリケーションソフトウェア部13との認証を行い、認証が成功した場合、PC内用暗号化手段7に暗号化の鍵を、アプリ認証手段8に復号化のための鍵を渡す手段である。署名メモリ4は、署名生成手段9で生成された署名を記録するメモリである。伝送解読手段6は、外部機器との認証に成功した場合、伝送認証手段2から鍵を受け取り、1394 D-I F1を介して入力されるAVデータを復号化する手段である。PC内用暗号化手段7は、伝送解読手段6で復号化されたAVデータを、アプリケーションソフトウェア部13との認証が成功した場合、再び暗号化し、そのデータをアプリケーション部13に渡す手段である。

## 【0028】

アプリケーションソフトウェア部13は、アプリ認証手段8、署名生成手段9、データ使用（デコード表示）手段10、解読手段11から構成される。

## 【0029】

アプリ認証手段 8 は、システム部 12 のアプリ認証関数と認証を行う手段である。署名生成手段 9 は、システム部 12 と認証を行うために用いるデジタル署名を生成する手段である。データ使用（デコード表示）手段 10 は、現在起動中のアプリケーションソフトウェアにその AV データを利用できるようにする手段である。解読手段 11 は、システム部 12 との認証が成功した場合、アプリ認証手段 9 から復号化のための鍵を入手し、その鍵を用いて PC 内用暗号化手段 7 で暗号化された AV データを復号化する手段である。

#### 【0030】

次にこのような本実施の形態の動作を説明する。

#### 【0031】

まず著作権情報の表し方について説明する。

#### 【0032】

STB や VTR 等の外部機器から AV データが PC 24 に送られてくる際、その AV データが著作権主張されている場合がある。すなわち、複製禁止や 1 回のみ複製を許可するなどの条件が付与されている場合がある。こういった利用許諾を表す信号情報は、ストリーム中に埋め込まれた CGMS (Copy Generation information) を用いて行われている。

#### 【0033】

CGMS は放送局から送られてくるトランスポートストリームの内部に存在している。CGMS は 2 ビットのデータであり、CGMS の取りうる値とその意味は次のようになる。

#### 【0034】

すなわち CGMS = 11 のとき copy never を意味し、CGMS = 10 のとき copy one generation を意味し、CGMS = 00 のとき copy free を意味する。また CGMS = 01 は存在しない。ただし copy never は複製禁止のことであり、その AV データを視聴することだけを許可する。copy one generation は 1 世代のみ複製を許可するものであり、複製した AV データは何度でも繰り返して視聴することが出来るものである。copy free は自由に複製してよいことを示すも

のである。CGMSを検出するためにはトランスポートストリームデコーダ回路などが必要になり、ハードウェア構成が複雑になる。

## 【0035】

一方、IEEE1394のパケットデータのヘッダ内に利用許諾情報を送るための信号情報（以下EMI (Encryption Mode Indicator) と記す）を付加することによって、トランスポートストリームデコーダ回路などのハードウェアは不要になる。

## 【0036】

EMIはCGMSから生成され、次の値をとる。すなわちEMI=11のときcopy neverを意味し、EMI=10のときcopy one generationを意味し、EMI=00のときcopy freeを意味する。またEMI=01はno more copyを意味する。ただしcopy neverは複製禁止のことであり、そのAVデータを視聴することだけを許可する。copy one generationは1世代のみ複製を許可するものであり、複製したAVデータは何度でも繰り返して視聴することができるものである。copy freeは自由に複製してよいことを示すものである。またno more copyはcopy one generationのAVデータを複製した後のAVデータであることを示し、これ以上の複製は不許可を表す。

## 【0037】

このようなEMIはIEEE1394では、暗号の方法、認証の方法を指定するのに用いられる。例えばEMI=00のcopy freeではAVデータを送る際に暗号化は行われず。またEMI=10のcopy one generationとEMI=01のno more copyでは、EMI=11のcopy neverと暗号化に用いられる鍵や機器の認証方法が異なる。

## 【0038】

今、STBからAVデータが送られてきたとする。そうするとSTBから送られてくるAVデータが著作権主張されているかどうかを前述したCGMSやEMIで判断し、著作権主張されている場合は、AVデータの送信元であるSTBと

認証を行う。AVデータは暗号化されて送られてきており、認証に成功すれば、伝送認証手段2はSTBからAVデータを復号化するための鍵を入手する。EMIが11の場合は公開鍵による認証が行われ、またEMIが10か01の場合は共通鍵による認証が行われる。

#### 【0039】

伝送認証手段とSTBの間で認証に成功すると、次にアプリケーションソフトウェア部13とシステム部12との間で認証を行うようにした。アプリ認証手段8は、署名生成手段9で、現在起動中のアプリケーションソフトウェアのデジタル署名を生成する。署名メモリ4は署名生成手段8で生成されたデジタル署名を記録する。アプリ認証関数3は、署名メモリ4に記録されているデジタル署名をもとにアプリ認証手段8との間で認証を行う。

#### 【0040】

ただし予めそれぞれのアプリケーションソフトウェアには、著作権主張されたAVデータの利用許諾情報に対応するライセンスを付与しておく。アプリケーションソフトウェア部13とシステム部12との認証によって正当なライセンスを有するソフトウェアのみ認証に成功するようにした。具体的には、アプリケーションソフトウェアの機能に応じてライセンスを分類する。AVデータの表示のみ行うソフトウェアに与えるライセンスをライセンスAとし、AVデータを記録するソフトウェアに与えるライセンスをライセンスBとする。さらに著作権主張された内容を厳守するソフトウェアのライセンスをCとする。ライセンスCは、AVデータが複製禁止の場合は、そのAVデータに対しては再生のみ行い、複製をせず、またAVデータが一回限り複製許可の場合は、そのAVデータに対しては一回限り複製を行うようなソフトウェアである。ただしライセンスCの場合、著作権主張されたAVデータの著作権の内容をAVデータとともにアプリケーションソフトウェアに通知する必要があるが、これはEMIまたはCGMSとしてAVデータに組み込んでおけばよい。

#### 【0041】

現在起動中のアプリケーションソフトウェアのライセンスが、Bであるとする。そして、STBから送られてきたAVデータの利用許諾情報は、EMIが11

であるとする。すなわちAVデータの複製は禁止されているとする。この場合、アプリ認証手段8とアプリ認証関数3との間で認証が行われるが、認証は成功しない。また現在起動中のアプリケーションソフトウェアのライセンスが、Aであるとする。この場合このアプリケーションソフトウェアは表示のみを行うソフトウェアであるので、アプリ認証手段8とアプリ認証関数3との間の認証が成功する。

さらにAVデータが複製禁止の場合、ライセンスCのアプリケーションソフトウェアである場合は、認証に成功する。AVデータの利用許諾の種類とアプリケーションソフトウェアのライセンスの種類と認証に成功するか失敗するかの一覧表を図7に示しておく。

#### 【0042】

アプリケーションソフトウェア部13とシステム部12との認証に成功した場合、伝送解読手段6は、伝送認証手段2から暗号解読用の鍵を受け取って、1394D-IF1を介して送られてくるAVデータを復号化する。次にPC内用暗号化手段7で、このAVデータを再び暗号化する。PC24内では、アプリケーションソフトウェアに使用される直前まで、著作権主張されたAVデータは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段10を構成する解読手段11は、アプリ認証手段8から暗号解読用の鍵を受け取り、AVデータを復号化する。復号化されたAVデータはデータ使用（デコード表示）手段10から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

#### 【0043】

またアプリケーションソフトウェア部13とシステム部12との認証に失敗した場合、伝送解読手段6がAVデータを復号化したのち、PC内用暗号化手段7で再び暗号化し、データ使用（デコード表示）手段10に送る。認証に失敗したためアプリ認証手段8はアプリ認証関数3から復号化のための鍵を受け取ることはできないので、解読手段11に復号化のための鍵を渡すことは出来ず、従って、解読手段11はAVデータを復号化することは出来ない。このようにライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、AVデータを復号化して処理することができない。



## 【0044】

このように、PC24の内部では、著作権主張されているAVデータを暗号化し、さらにシステム部12とアプリケーションソフトウェア部13との間で認証を行い、ライセンスを受けているアプリケーションソフトウェアを選別することによって、ライセンスを受けていないアプリケーションソフトウェアがAVデータを受け取っても、データが暗号化されているためにそのAVデータを意味ある物として使用することができず、著作権主張されたAVデータを守ることができる。

## 【0045】

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されているAVデータを復号化せず、そのままPCの内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

## 【0046】

さらに本実施の形態のPC内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全にAVデータの著作権を守ることが出来る。

## 【0047】

さらに本発明のシステム部は、1394D-I Fを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、PC内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

## 【0048】

さらに本実施の形態のライセンスは上述したようにA、B、Cの3種類に分けるものに限らない。4種類や2種類など、要するに、AVデータの著作権情報の

種類に対応する分け方でありさえすればよい。

【0049】

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送ることのできる機器であればなんでもよい。

【0050】

さらに、本実施の形態ではIEEE1394を例にあげて説明したが、これに限らず、著作権主張されたAVデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

【0051】

さらに本実施の形態のAVデータは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

【0052】

さらに本実施の形態のPCは本発明のコンピュータの例である。

【0053】

(実施の形態2)

次に第2の実施の形態について図2を参照して説明する。

【0054】

本実施の形態では、システム部とアプリケーションソフトウェア部とで認証を行う前に不正なまたは正当なアプリケーションソフトウェアを示す管理基準（以下CRLと呼ぶ）によってアプリケーションソフトウェアを判定しておく場合を説明する。

【0055】

第1の実施の形態との相違点は、システム部12がCRLメモリ14、アプリケーションCRLメモリ15、CRL比較手段16を有する点である。以下第1の実施の形態との相違点を中心に説明する。

## 【0056】

CRLメモリ14は、不正なまたは正当な機器を示す管理基準を記憶するメモリである。またアプリ用CRLメモリ15は、不正なまたは正当なアプリケーションソフトウェアを示す管理基準を記憶する手段である。CRL比較手段16はCRLによってアプリケーションソフトウェアが不正か正当かを判断する手段である。

## 【0057】

次にこのような本実施の形態の動作を説明する。

## 【0058】

本実施の形態でもSTBからAVデータが送られてくるとし、そのAVデータは著作権主張されているとする。まず第1に伝送解読手段6とSTBの間で認証を行う前にSTBのCRLメモリに記憶されているCRLを用いてPC24が正当な機器か不正な機器かの判定がなされる。正当な機器と判定されれば、伝送認証手段2がSTBとの認証を行う。不正な機器と判定されればSTBは認証を行わず、暗号化されているAVデータを復号化する鍵をPC24に渡さない。

## 【0059】

今、PC24はSTBによって正当な機器と判定されたとする。そうすると伝送認証手段2が1394D-IF1を介してSTBと認証を行う。認証が成功すれば、STBはAVデータを復号化するための鍵を1394D-IF1を介して、伝送認証手段2に渡す。

## 【0060】

次に署名生成手段9は、現在起動しているアプリケーションソフトウェアのデジタル署名を作成し、署名メモリ4が記憶する。CRL比較手段16は署名メモリ4に記憶されているデジタル署名の内容と、アプリ用CRLメモリ15の内容を比較し、現在起動中のアプリケーションソフトウェアが不正なソフトウェアか正当なソフトウェアかどうかを判定する。不正なソフトウェアである場合は、アプリケーションソフトウェア部13とシステム部12との認証を行わない。また正当なソフトウェアである場合は、次にアプリケーションソフトウェア部13とシステム部12との間で認証を行うようにした。ただしアプリケーションソ

フトウェアには第1の実施の形態と同様のライセンスが付与されているとする。

【0061】

ここで、アプリ用CRLメモリ15は、PC24内のOSやドライバ等のメモリであって、独自に予め作成したCRLを記憶しておいてもよいし、IEEE1394から送られてくるCRLを流用してもよい。このCRLは一般に固定されたものではなく、状況に応じて更新することが出来る。例えば機器やアプリケーションが著作権を侵害するように改変され流通した場合に、それらを特定して認証を失敗させるよう、CRLを更新することが可能である。

【0062】

アプリケーションソフトウェア部13とシステム部12との認証に成功した場合、伝送解読手段6は、伝送認証手段2から暗号解読用の鍵を受け取って、1394D-I/Fを介して送られてくるAVデータを復号化する。次にPC内用暗号化手段7で、このAVデータを再び暗号化する。PC24内では、アプリケーションソフトウェアに使用される直前まで、著作権主張されたAVデータは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段10を構成する解読手段11は、アプリ認証手段8から暗号解読用の鍵を受け取り、AVデータを復号化する。復号化されたAVデータはデータ使用（デコード表示）手段10から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

【0063】

またアプリケーションソフトウェア部13とシステム部12との認証に失敗した場合、伝送解読手段6がAVデータを復号化したのち、PC内用暗号化手段7で再び暗号化し、データ使用（デコード表示）手段10に送る。認証に失敗したためアプリ認証手段8は復号化のための鍵を解読手段11に渡すことは出来ず、従って、解読手段11はAVデータを復号化することは出来ない。従ってライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、AVデータを処理することができない。

【0064】

あるいは、アプリ用CRLメモリ15から、破られ無効になったタンパレジスタンス方式のバージョン情報を入手し、アプリケーションが無効となったバージ

ョンしか持たない場合には、アプリ認証関数3にAVデータを復号するための鍵を渡さず、システム部12とアプリケーションソフトウェア部13との認証も行わない。

【0065】

このように、アプリケーションソフトウェア部とシステム部で認証する前にCRLを用いて現在起動中のアプリケーションソフトウェアが不正か正当かを判断することによって、著作権主張されたAVデータに対して、不正な動作を行うアプリケーションソフトウェアを予め排斥することができる。

【0066】

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されているAVデータを復号化せず、そのままPCの内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

【0067】

さらに本実施の形態のPC内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全にAVデータの著作権を守ることが出来る。

【0068】

さらに本発明のシステム部は、1394D-I Fを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、PC内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

【0069】

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外

部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送ることのできる機器であればなんでもよい。

【0070】

さらに、本実施の形態ではIEEE1394を例にあげて説明したが、これに限らず、著作権主張されたAVデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

【0071】

さらに本実施の形態のAVデータは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

【0072】

さらに本実施の形態のPCは本発明のコンピュータの例である。

【0073】

(実施の形態3)

次に第3の実施の形態について図3を参照して説明する。

【0074】

本実施の形態ではタンパ認証関数を用いてアプリケーションソフトウェアが不正に改竄されているかどうかを判定する場合を説明する。

【0075】

第1の実施の形態との相違点は、システム部12がタンパ認証関数17を有し、またアプリケーションソフトウェア部13がソフトチェック手段18を有する点である。

【0076】

タンパ認証関数17は、アプリケーションソフトウェアから発生するタンパコードを検証し、アプリケーションソフトウェアが改竄されていないかどうかの確認を行う手段である。ソフトチェック手段18は、現在起動しているアプリケーションをチェックし、タンパコードを発生させる手段である。

【0077】

次にこのような本実施の形態の動作を説明する。

【0078】

上述したようにタンパコードを発生するタンパレジスタントソフトウェアとは、内部解析や改変に対して耐性を備えているソフトウェアである。すなわち著作権主張されたAVデータを不正に利用しようとする悪意を持つユーザの攻撃があっても、防御できるようにしたソフトウェアである。タンパレジスタントソフトウェアはタンパコードと呼ばれるコードを発生する。ソフトチェック手段18はプログラムを調べて改竄の有無を検証し、さらに実行環境を調べてデータ経路での傍受の有無やプログラムの実行を監視する第3者の存在などを検証する。タンパコードとはこの検証の結果か、または中間結果を表すデータである。このコードを検証することによって、タンパレジスタントソフトウェアが改竄されていないかどうかを確認することができる。つまり本実施の形態ではアプリケーションソフトウェアはタンパレジスタントの方式を実装しているものとする。

【0079】

第1の実施の形態と同様にSTBと伝送認証手段2との間で認証が行われ、認証が成功したものとする。そうすると、ソフトチェック手段18は、現在起動中のアプリケーションソフトウェアをチェックし、タンパコードを発生させる。発生したタンパコードは、アプリ認証手段に渡され、さらに署名生成手段9で、デジタル署名に書き込まれ、このデジタル署名は署名メモリ4に記憶される。タンパ認証関数17は、署名メモリ4に記憶されているデジタル署名を参照し、現在起動しているアプリケーションソフトウェアのタンパコードを取り出し、検証する。その結果現在起動しているアプリケーションが不正に改竄されていないか、データの傍受やプログラムの実行の監視が行われていないかどうかの判定結果をアプリ認証関数3に通知する。以下、簡単のため、データの傍受やプログラムの実行の監視が行われていないかどうかの判定もアプリケーションが不正に改竄されて居ないかの判定に含まれることとして説明する。アプリ認証関数3はアプリケーションソフトウェアが不正に改竄されている場合、アプリ認証手段8にAVデータを復号化するための鍵を渡さず、システム部12とアプリケーションソフトウェア部13との認証も行わない。また不正に改竄されていない場合は

、アプリ認証関数 3 とアプリ認証手段 8 は、署名メモリ 4 に記録されているデジタル署名をもとに認証を行う。ただし第 1 の実施の形態と同様にアプリケーションソフトウェアにはライセンスが付与されている。認証が成功すると、アプリ認証関数 3 は AV データを復号化するための鍵をアプリ認証手段 8 に渡す。

#### 【0080】

アプリケーションソフトウェア部 13 とシステム部 12 との認証に成功した場合、伝送解読手段 6 は、伝送認証手段 2 から暗号解読用の鍵を受け取って、1394 D-I F1 を介して送られてくる AV データを復号化する。次に PC 内用暗号化手段 7 で、この AV データを再び暗号化する。PC 24 内では、アプリケーションソフトウェアに使用される直前まで、著作権主張された AV データは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段 10 を構成する解読手段 11 は、アプリ認証手段 8 から復号化用の鍵を受け取り、AV データを復号化する。復号化された AV データはデータ使用（デコード表示）手段 10 から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

#### 【0081】

またアプリケーションソフトウェア部 13 とシステム部 12 との認証に失敗した場合、伝送解読手段 6 が AV データを復号化したのち、PC 内用暗号化手段 7 で再び暗号化し、データ使用（デコード表示）手段 10 に送る。認証に失敗したためアプリ認証手段 8 は復号化のための鍵を解読手段 11 に渡すことは出来ない。従って解読手段 11 は AV データを復号化することは出来ない。従ってライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、AV データを処理することができない。

#### 【0082】

このようにアプリケーションソフトウェアにタンパレジスタントの方式を実装し、さらにアプリケーションソフトウェアが不正に改竄されていないかどうかを確認する機能を付加することによってより確実に AV データの著作権を守ることができる。

#### 【0083】

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わ



ないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されているＡＶデータを復号化せず、そのままＰＣの内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

## 【００８４】

さらに本実施の形態のＰＣ内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全にＡＶデータの著作権を守ることが出来る。

## 【００８５】

さらに本発明のシステム部は、１３９４Ｄ－ＩＦを構成するハードウェアまたはドライバやＯＳなどのシステムソフトウェアでも実現可能である。要するに、ＰＣ内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

## 【００８６】

さらに本実施の形態では外部機器としてＳＴＢを例にあげて、ＳＴＢから著作権主張されたＡＶデータをＰＣが受けとるとして説明したが、これに限らず、外部機器としてＤＶＣ、ＤＶＨＳ、ＨＤＤ、ＤＶＤ－ＲＡＭ、放送受信機など、要するに著作権主張されたＡＶデータを送ることのできる機器であればなんでもよい。

## 【００８７】

さらに、本実施の形態ではＩＥＥＥ１３９４を例にあげて説明したが、これに限らず、著作権主張されたＡＶデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

## 【００８８】

さらに本実施の形態のＡＶデータは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデー

タでありさえすればよい。

【0089】

さらに本発明のタンパコード及びタンパレジスタンス確認関数は、タンパレジスタントの方式によらず、任意のタンパレジスタントの方式を用いることができる。

【0090】

さらに本実施の形態のPCは本発明のコンピュータの例であり、本実施の形態のタンパ認証関数は本発明のタンパレジスタンス確認関数の例である。

【0091】

(実施の形態4)

次に第4の実施の形態について図4を参照して説明する。

【0092】

本実施の形態ではタンパ認証関数を用いてアプリケーションソフトウェアが不正に改竄されているかどうかを判定する場合を説明する。

【0093】

第3の実施の形態との相違点は、システム部12が複数種類のタンパ認証関数21を有し、またバージョン選択手段20を有し、またアプリケーションソフトウェア部13のソフトチェック手段19がタンパコードに加えてアプリケーションソフトウェアに実装しているタンパレジスタントの方式の種類情報を発生する点である。

【0094】

バージョン選択手段20は、署名メモリ4に記録されているデジタル署名をもとにタンパレジスタントの方式の種類に対応するタンパ認証関数を選択する手段である。

【0095】

次にこのような本実施の形態の動作を説明する。

【0096】

第3の実施の形態と同様、アプリケーションソフトウェアはタンパレジスタントの方式を実装しているとする。第3の実施の形態と同様にSTBと伝送認証手

段 2 とで認証が行われ、認証が成功したものとする。そうすると、ソフトチェック手段 19 は、現在起動中のアプリケーションソフトウェアをチェックし、タンパコードと実装しているタンパレジスタントの方式の種類情報を発生させる。発生したタンパコードと種類情報は、アプリ認証手段 8 に渡され、さらに署名生成手段 9 で、デジタル署名に書き込まれ、このデジタル署名は署名メモリ 4 に記憶される。バージョン選択手段 20 は、署名メモリ 4 に記憶されているタンパレジスタントの方式の種類情報を参照し、使用するタンパ認証関数を選択する。この際、バージョン選択手段 20 は、図では省略するがタンパバージョンに関する独自の CRL メモリを備えているものとし、この CRL メモリを利用する事で、既に破る方法が知られているタンパレジスタンスチェック手段 19 を選択しないという動作を行う。選択されたタンパ認証関数 21 は、署名メモリ 4 に記憶されているデジタル署名を参照し、現在起動しているアプリケーションソフトウェアのタンパコードを取り出し、検証する。その結果現在起動しているアプリケーションソフトウェアが不正に改竄されていないかどうかの判定結果をアプリ認証関数 3 に通知する。アプリ認証関数 3 はアプリケーションソフトウェアが不正に改竄されている場合、アプリ認証手段 8 に A V データを復号化するための鍵を渡さず、システム部 12 とアプリケーションソフトウェア部 13 との認証も行わない。また不正に改竄されていない場合は、アプリ認証関数 3 とアプリ認証手段 8 は、署名メモリ 4 に記録されているデジタル署名をもとに認証を行う。ただし第 1 の実施の形態と同様にアプリケーションソフトウェアにはライセンスが付与されている。認証が成功すると、アプリ認証関数 3 は A V データを復号化するための鍵をアプリ認証手段 8 に渡す。

#### 【0097】

アプリケーションソフトウェア部 13 とシステム部 12 との認証に成功した場合、伝送解読手段 6 は、伝送認証手段 2 から暗号解読用の鍵を受け取って、1394 D-I F 1 を介して送られてくる A V データを復号化する。次に P C 内用暗号化手段 7 で、この A V データを再び暗号化する。P C 24 内では、アプリケーションソフトウェアに使用される直前まで、著作権主張された A V データは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段 10 を構成す

る解読手段 11 は、アプリ認証手段 8 から復号化用の鍵を受け取り、A V データを復号化する。復号化された A V データはデータ使用（デコード表示）手段 10 から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

【0098】

またアプリケーションソフトウェア部 13 とシステム部 12 との認証に失敗した場合、伝送解読手段 6 が A V データを復号化したのち、P C 内用暗号化手段 7 で再び暗号化し、データ使用（デコード表示）手段 10 に送る。認証に失敗したためアプリ認証手段 8 は復号化のための鍵を解読手段 11 に渡すことは出来ず、解読手段 11 は A V データを復号化することは出来ない。従ってライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、A V データを処理することができない。

【0099】

このようにアプリケーションソフトウェアにタンパレジスタントの方式を実装するのみならず、複数のタンパレジスタント認証関数をシステム部に実装することにより、アプリケーションソフトウェアのタンパレジスタントの方式が例え破られたとしても、システム部はタンパレジスタント認証関数を別の種類に切り替えるだけですみ、O S のバージョンアップなどを行う必要がないので、タンパレジスタントの方式が破られたことによる被害を最小限に抑えることができる。

【0100】

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されている A V データを復号化せず、そのまま P C の内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

【0101】

さらに本実施の形態の P C 内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わな

い。このようにすることによってより安全にAVデータの著作権を守ることが出来る。

【0102】

さらに本発明のシステム部は、1394D-I Fを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、PC内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

【0103】

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送ることのできる機器であればなんでもよい。

【0104】

さらに、本実施の形態ではIEEE1394を例にあげて説明したが、これに限らず、著作権主張されたAVデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

【0105】

さらに本実施の形態のAVデータは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

【0106】

さらに本発明のタンパコード及びタンパレジスタンス確認関数は、タンパレジスタントの方式によらず、任意のタンパレジスタントの方式を用いることができる。

【0107】

さらに本実施の形態のPCは本発明のコンピュータの例であり、本実施の形態のタンパ認証関数は本発明のタンパレジスタンス確認関数の例である。

【0108】

## (実施の形態 5)

次に第 5 の実施の形態について図 5 を参照して説明する。

## 【0109】

本実施の形態では、AV データを処理するアプリケーションソフトウェアに関する情報を電子透かしによって AV データに埋め込む場合を説明する。

## 【0110】

ここでいう電子透かしとは署名などのデータを AV データに改変が困難なように織り込むための技術を指すこととし、アナログ的なデータ重畳に基づくものか、デジタル的に暗号技術に基づくものかなどは問わない。

## 【0111】

第 1、2 の実施の形態との相違点は、システム部に署名埋め込み手段 22、電子透かし埋め込み手段 23 を有している点である。

## 【0112】

署名埋め込み手段 22 は、署名メモリ 4 に記録されているデジタル署名の内容を参照し、電子透かし埋め込み手段 23 で必要な情報を選別し、書式を整えるなどの電子透かし埋め込み手段 23 の前処理を行う手段である。電子透かし埋め込み手段 23 は、署名埋め込み手段 22 で整えられた書式で、AV データに電子透かしによるデータの埋め込みを行う手段である。

## 【0113】

本実施の形態のうち伝送認証手段 2、アプリ認証関数 3、署名メモリ 4、アプリ認証手段 8、署名生成手段 9、伝送解読手段 6、PC 内用暗号化手段 7、データ使用（デコード表示）手段 10、解読手段 11 は、第 1 の実施の形態と同じである。また CRL メモリ 14、アプリ用 CRL メモリ 15、CRL 比較手段 16 は、第 2 の実施の形態と同じである。

## 【0114】

次にこのような本実施の形態の動作を説明する。

## 【0115】

外部の機器、例えば STB と伝送認証手段 2 と認証を行い成功したとする。さらにアプリ認証手段 8 とアプリ認証関数 3 の間での認証も成功したとする。そう

すると1394D-IF1から入力された暗号化されているAVデータは伝送解読手段6で復号化される。署名埋め込み手段22は、署名メモリ4よりアプリケーションソフトウェアの情報を含んだデジタル署名を取り出し、内容を選別する。選別される内容は、アプリケーションソフトウェアのソフト名、アプリケーションソフトウェアのバージョン番号、使用者に関する情報、AVデータ自身の情報である。署名埋め込み手段22は、これらの情報に書式を整える等の前処理を施し、電子透かし埋め込み手段23に送る。電子透かし埋め込み手段23は、復号化されたAVデータ自身にこれらの情報の電子透かしを作成する。電子透かしを作成されたAVデータはPC内用暗号化手段7で再び暗号化され、データ使用（デコード表示）手段10に渡される。解読手段11がAVデータを復号化し、データ使用（デコード表示手段）10が現在起動中のアプリケーションソフトウェアにそのAVデータを渡す。AVデータを受け取ったアプリケーションソフトウェアは表示、記録、再生などの処理を行う。

## 【0116】

ここで、アプリケーションソフトウェアが電子透かしを施されたAVデータを不正に記録し、PC24の外部に配布したとする。この不正に配布されたAVデータは、AVデータのCGMSやEMIが不正なアプリケーションによって書き替えられてしまったとする。そうすると、正当な機器でも記録できるようになり、このAVデータは様々な機器に流出していく。このように不正に流出していったAVデータをチェックする管理機関がこのAVデータを入手すれば、AVデータに埋め込まれた電子透かしを参照することにより以下のことがわかる。すなわち、AVデータの情報からそのAVデータが記録禁止等であることがわかり、またそのAVデータを不正に複製、配布したアプリケーションソフトウェアに関する情報がわかり、出所のアプリケーションソフトウェアを特定することができる。

## 【0117】

このように本発明では不正配布の出所に関する情報を特定できるが、さらに本発明のコンピュータは、CRLを更新する手段を備えているため、前記の出所に関する情報に基づいてCRLを更新することで、不正配布を行ったアプリケーシ

ョンを、以後AVデータの利用から排除し、そのことにより以後の不正利用を防止する具体的手段を提供する。このように電子透かしを用いることにより不正な複製の出所を特定し、容易に不正なアプリケーションソフトウェアを特定することができる。

#### 【0118】

なお、電子透かしの方式は本実施の形態で用いたものに限らず、AVデータ内に正しく前述の情報を埋め込むことが出来、所定の形式によりデコード前あるいはデコード後にAVデータから前述の情報が正しく抽出出来るものであればどのような方式のものを用いても構わない。

#### 【0119】

このように、AVデータに電子透かしを埋め込むことによって、不正なアプリケーションソフトウェアを容易に特定し、排斥することができるようになる。

#### 【0120】

##### (実施の形態6)

次に第6の実施の形態について図6を参照して説明する。

#### 【0121】

本実施の形態のPCは以上第1～第5の実施の形態で説明したすべてのPCの機能を備えるものである。

#### 【0122】

伝送認証手段2、アプリ認証関数3、署名メモリ4、アプリ認証手段8、署名生成手段9、伝送解読手段6、PC内用暗号化手段7、データ使用（デコード表示）手段10、解読手段11は第1の実施の形態で説明したものと同様である。また、CRLメモリ14、アプリ用CRLメモリ15、CRL比較手段16は第2の実施の形態で説明したのと同様である。またバージョン選択手段20、タンパ認証関数21は、第4の実施の形態で説明したのと同様である。また署名埋め込み手段22、電子透かし埋め込み手段23は第5の実施の形態で説明したのと同様である。

#### 【0123】

このように構成することにより、第1～第5の各実施の形態で説明した機能が



全て含まれているので、タンパレジスタントの採用によるソフトウェアの信頼性のチェックと、電子透かしによる確実な不正検出方式と、不正検出した際の再発防止手段を備えることで、著作権主張されたAVデータの不正利用防止が確実に行え、かつタンパレジスタント方式に対するバージョンの採用により不正利用の際の2次被害を最小限に限定出来るという効果が得られる。

#### 【0124】

なお、本発明のコンピュータの各構成要素の一部または全部の機能をコンピュータに実行させるためのプログラムを記録したことを特徴とするプログラム記録媒体も本発明に属する。

#### 【0125】

##### 【発明の効果】

以上説明したところから明らかなように、本発明は、著作権主張されたデータに対してはアプリケーションソフトウェアが著作権を守り、アプリケーションソフトウェアの不正な改竄に対抗することが出来、不正なアプリケーションソフトウェアに対して、そのアプリケーションソフトウェアを確認し、排斥することが出来、不正な流出をコストをかけずに排除する事が出来るコンピュータ及びプログラム記録媒体を提供することが出来る。

##### 【図面の簡単な説明】

#### 【図1】

本発明の第1の実施の形態におけるシステム部とアプリケーションソフトウェア部が認証を行い、AVデータはPC内で暗号化される場合のブロック図。

#### 【図2】

本発明の第2の実施の形態におけるCRLを用いて不正なアプリケーションソフトウェアを検出する場合のブロック図。

#### 【図3】

本発明の第3の実施の形態におけるタンパレジスタントの方式を実装した場合のブロック図。

#### 【図4】

本発明の第4の実施の形態における複数種類のタンパ認証関数を実装した場合

のブロック図。

【図5】

本発明の第5の実施の形態における著作権主張されたAVデータに電子透かしを埋め込む場合のブロック図。

【図6】

本発明の第6の実施の形態におけるより確実に著作権主張されたAVデータの著作権をまもることができる場合のブロック図。

【図7】

本発明の第1の実施の形態におけるアプリケーションソフトウェアのライセンスの種類によって認証が成功するか失敗するかを示した一覧図。

【符号の説明】

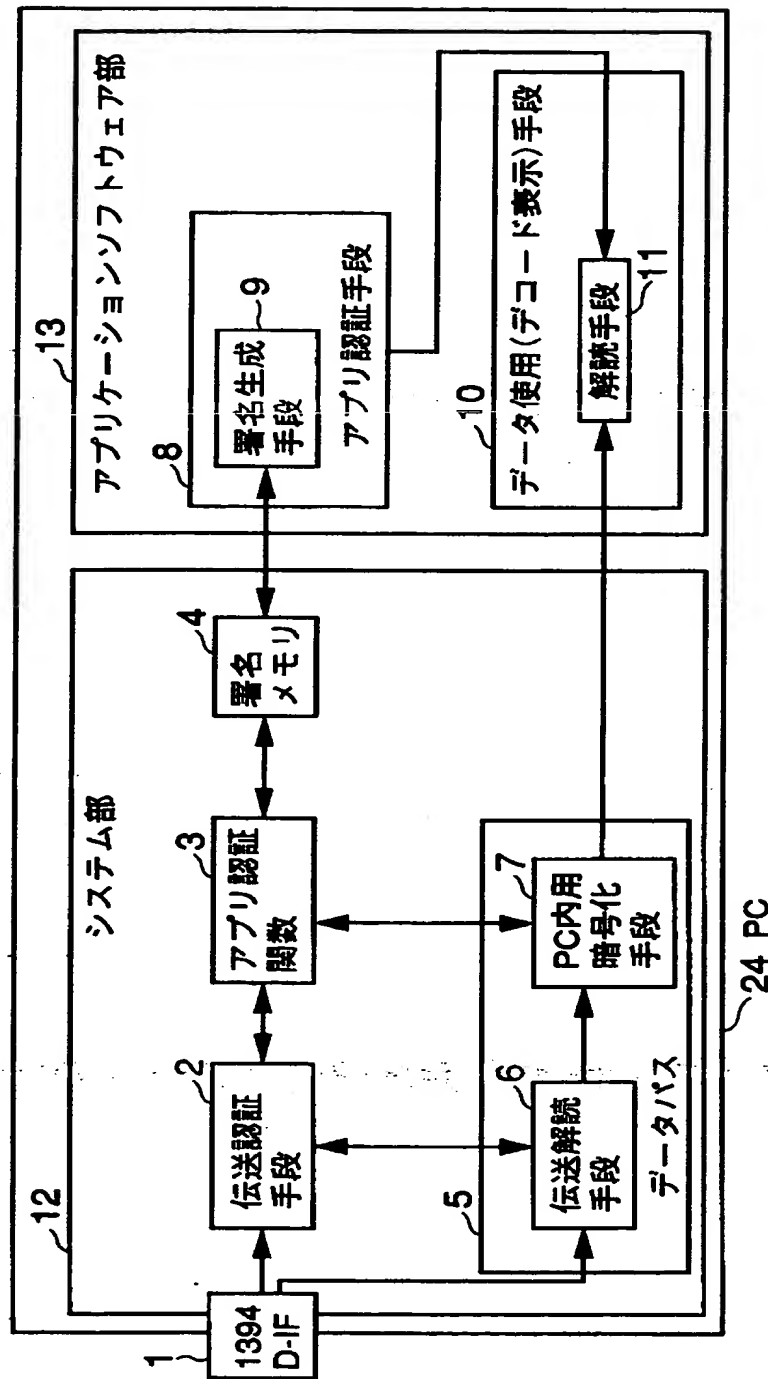
- 1 1394D-I F
- 2 伝送認証手段
- 3 アプリ認証関数
- 4 署名メモリ
- 5 データバス
- 6 伝送解読手段
- 7 PC内用暗号化手段
- 8 アプリ認証手段
- 9 署名生成手段
- 10 データ使用（デコード表示）手段
- 11 解読手段
- 12 システム部
- 13 アプリケーションソフトウェア部
- 14 CRLメモリ
- 15 アプリ用CRLメモリ
- 16 CRL比較手段
- 17 タンバ認証関数
- 18 ソフトチェック手段

- 19 ソフトチェック手段
- 20 バージョン選択手段
- 21 タンパ認証関数
- 22 署名埋込手段
- 23 電子透かし埋込手段

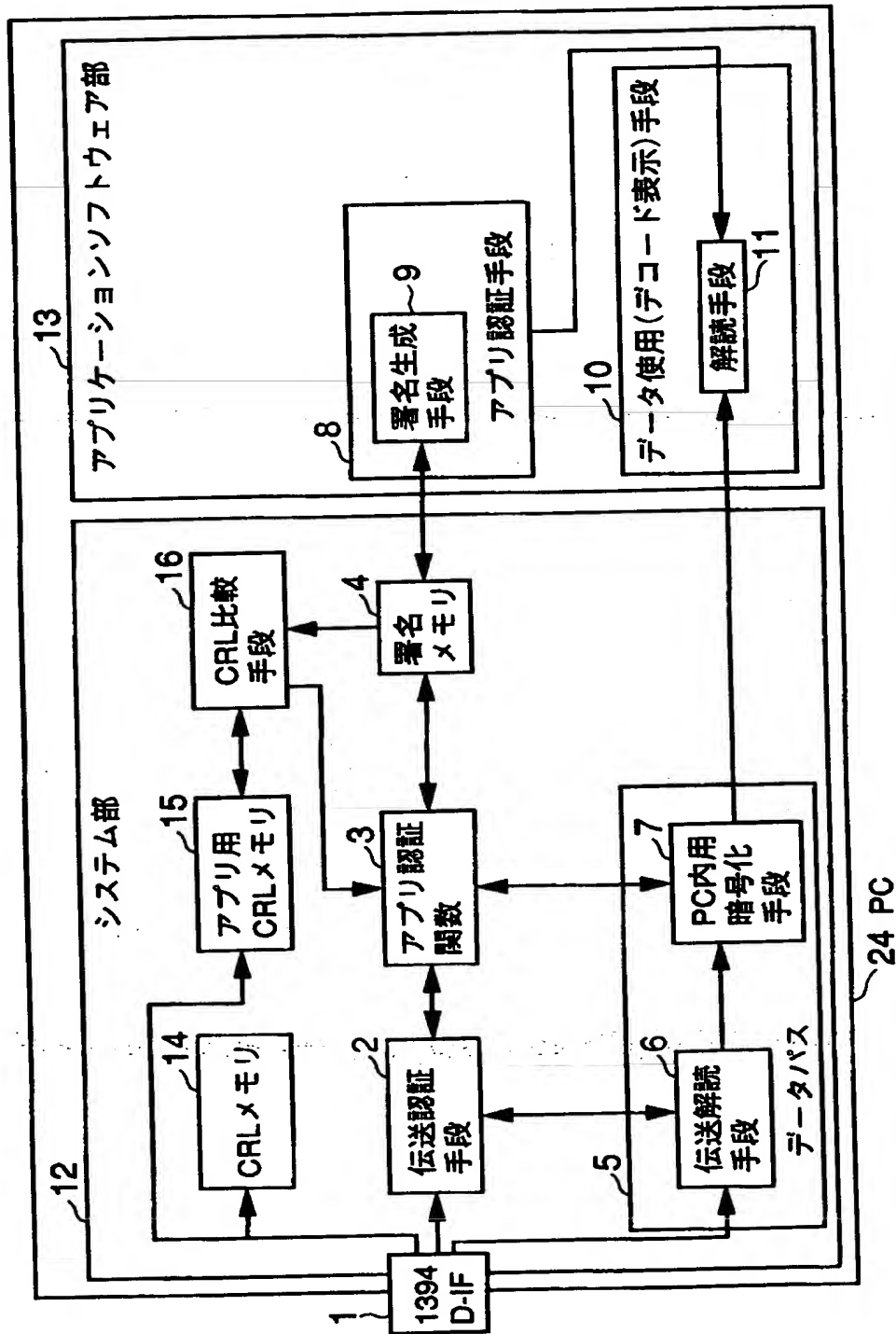
【書類名】

図面

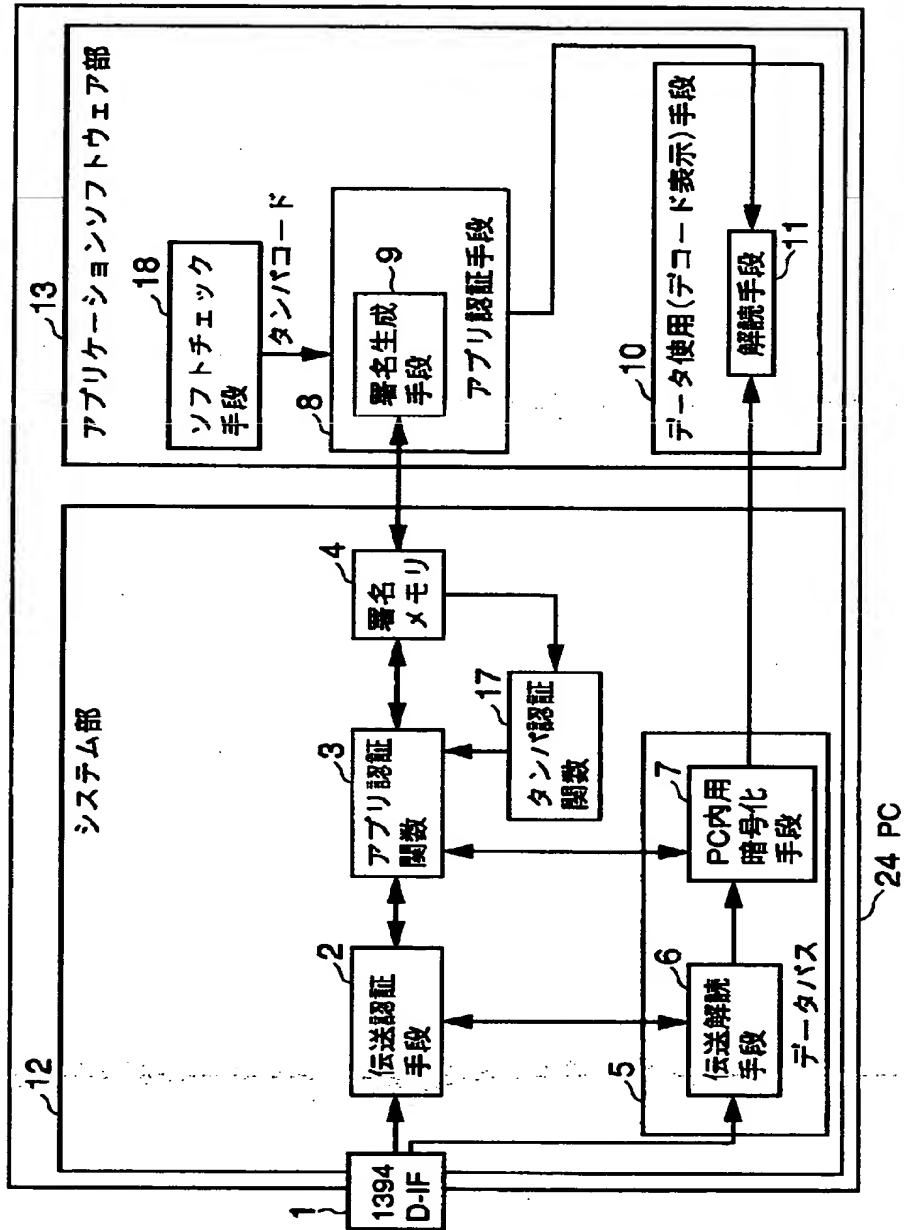
【図 1】



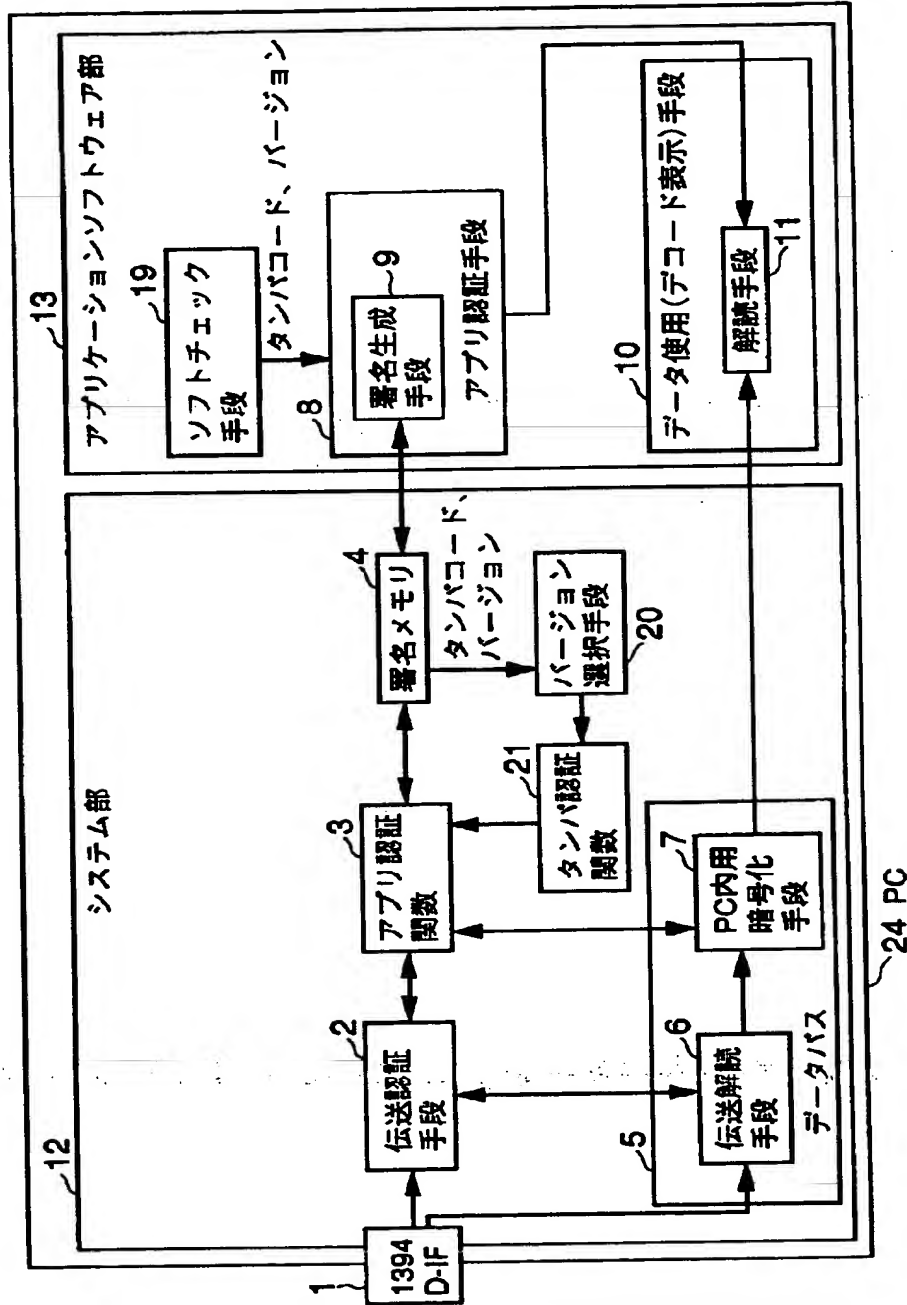
【図 2】



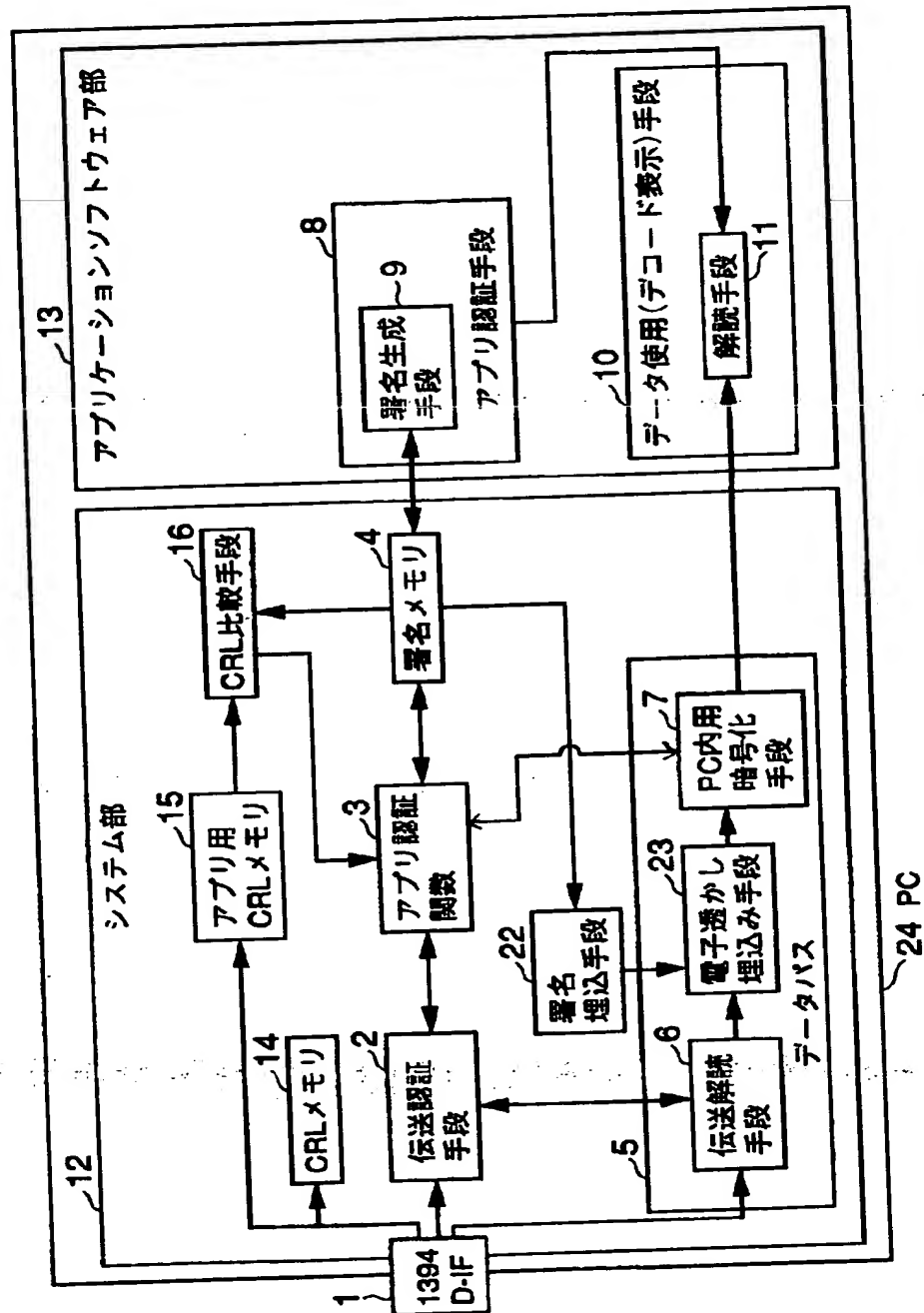
【図 3】



【図 4】

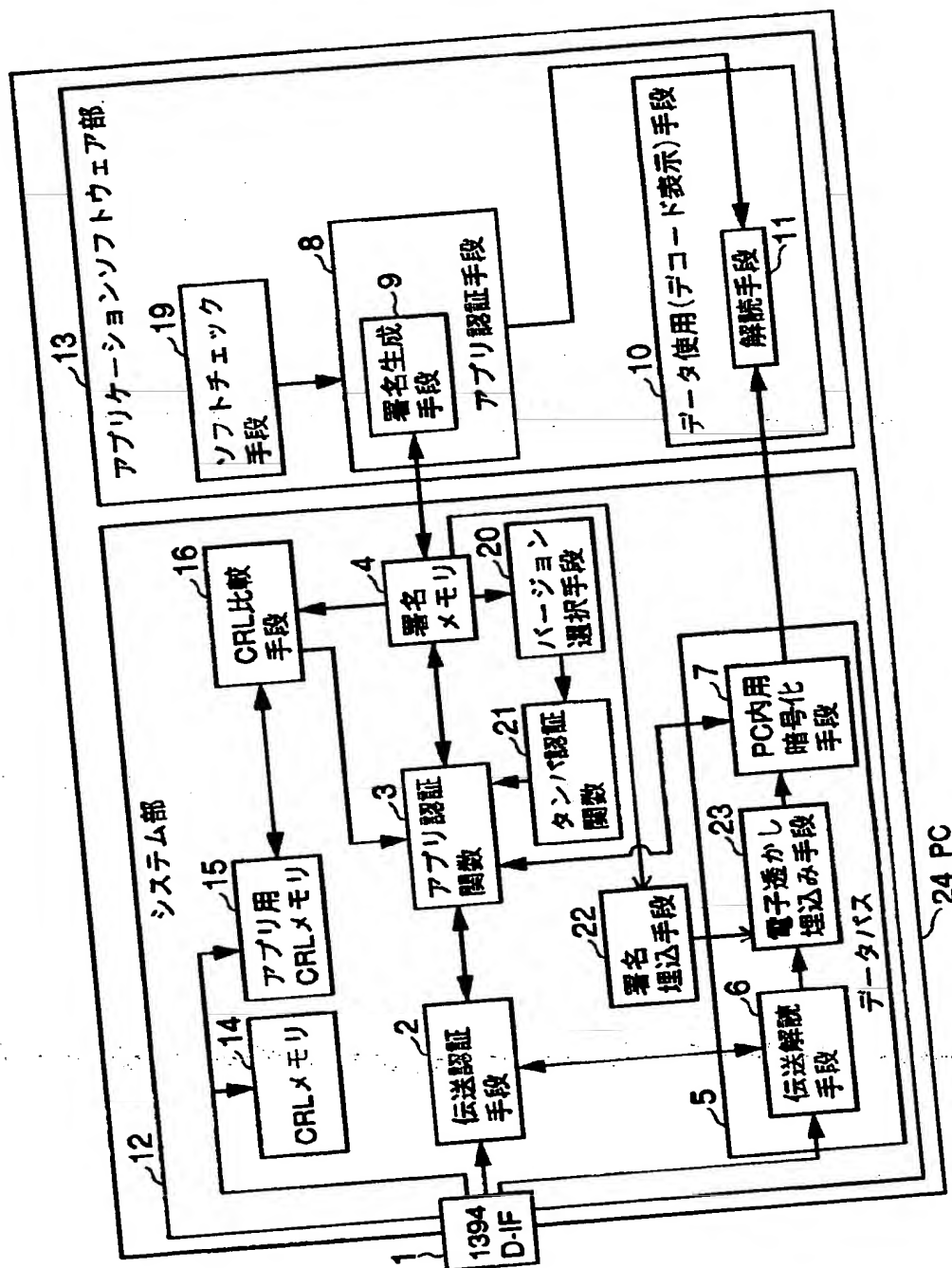


【図 5】





【図6】



【図 7】

| AVデータの著作権   | アプリケーション<br>ソフトウェアのライセンス | 認証 |
|-------------|--------------------------|----|
| 複製禁止        | A                        | 成功 |
| 複製禁止        | B                        | 失敗 |
| 複製禁止        | C                        | 成功 |
| 一回のみ複製許可    | A                        | 成功 |
| 一回のみ複製許可    | B                        | 失敗 |
| 一回のみ複製許可    | C                        | 成功 |
| これ以上の複製は不許可 | A                        | 成功 |
| これ以上の複製は不許可 | B                        | 失敗 |
| これ以上の複製は不許可 | C                        | 成功 |

【書類名】 要約書

【要約】

【課題】 著作権主張されたAVデータが一旦アプリケーションソフトウェアに渡されてしまえば、アプリケーションソフトウェアが自由にAVデータを記録などの処理をすることが可能であり、著作権を守ることが出来ないという課題がある。

【解決手段】 システム部12とアプリケーションソフトウェア部13とを備え、デジタルインターフェース1から著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、システム部12は、アプリケーションソフトウェア部13が著作権を守る上において正当なアプリケーションソフトウェアであると判定し、正当なものである場合は、暗号化データの鍵をアプリケーションソフトウェア部13に渡すことを特徴とするコンピュータ。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号

[000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社